deepwatch

Bridging the Cybersecurity Skills Gap in Security Operations

PRACTICAL STAFFING STRATEGIES FOR SECURITY LEADERS

Table of Contents

Introduction

There are currently 359,000 unfilled/open IT Security Jobs in the U.S. Globally, the shortage of cybersecurity professionals is estimated to be 2.72 Million[1]. The challenges with recruiting, hiring, and retaining experienced security personnel have reached a whole new, maddening level, driven by a system straining to fill a vast number of security positions with an insufficient talent pool. Staff turnover, high salaries, recruiting issues, and lean budgets all contribute to this perfect storm.

An added challenge faced by security leaders is that, despite advanced security tools and technologies, the lack of experienced security staff hinders most organizations from realizing the full capabilities of these technologies. It also means they're unable to sufficiently manage their risks in order to securely scale along with business growth.

The most recent study revealed a critical finding:

"Two-thirds of study participants report a cybersecurity staffing shortage is placing their organizations at risk."[2] This shortage is often referred to as the **cybersecurity skills gap**, and it means that in-house security teams often work extra hours and give up vacations and holidays[2] just to stay marginally on top of their workloads.

The long working hours and increasing threat pressures placed on IT security decisions makers and teams will not be sustainable at this pace.

In this eBook, you'll find actionable guidance to help make the case for security program funding to gain these benefits:

- **An improved security staffing process** that meets the organization's need for skilled personnel within budget.
- **A fully optimized security operations center** that supports growth, is secure against threats, and facilitates security in cloud, hybrid, and multi-cloud environments.
- **A risk management mechanism** to mitigate security risks associated with technology and staffing the security operations functions to secure the increasingly distributed enterprise.

Security Staffing
Is a Never-Ending Task

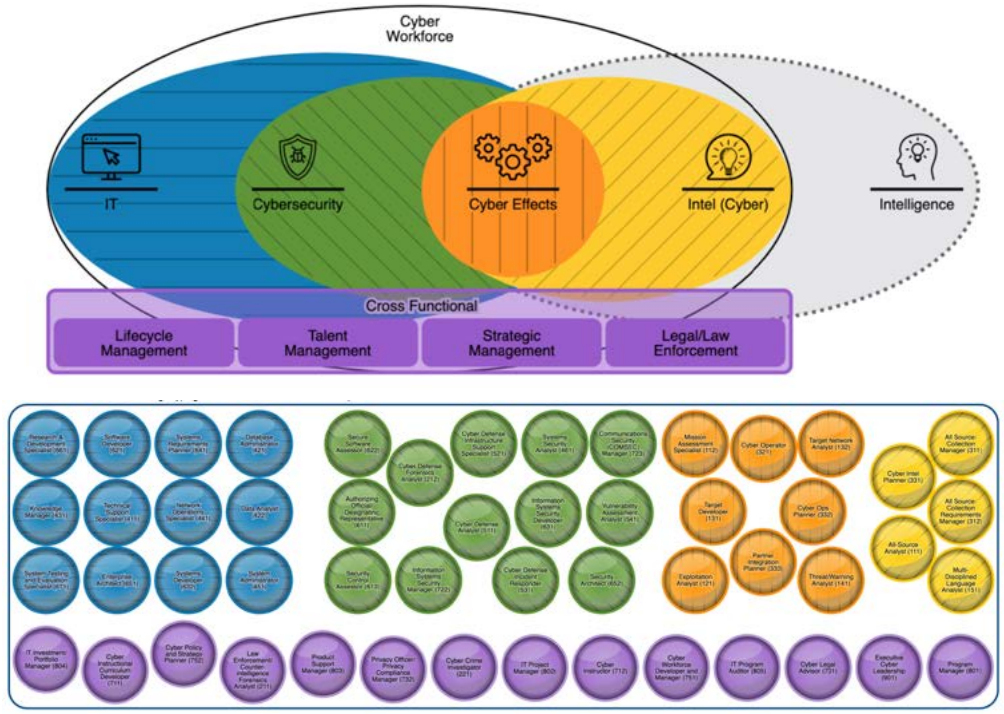
Whether you're staffing a Security Operations Center (SOC) or fully integrating a SecOps program into the organization, security teams need a full complement of experienced staff available 24/7/365. They can manage the security risks facing today's businesses and provide adequate protection against an evolving and sophisticated threat environment.

Three key facts underscore the criticality of staffing challenges in the current environment:

1. **Recruiting and hiring SecOps staff**, particularly personnel skilled in security event detection, threat hunting, and incident response, is an incredibly difficult undertaking for many organizations, since the skill sets are less common and in high-demand.

2. **Cybersecurity practitioners experience alert fatigue** when an overwhelming number of security alerts are firing from disparate security technologies, causing desensitization and staff burnout. If a real security event is lost in millions of daily alerts, a threat actor can lurk longer in the network, increasing 'dwell time.' The longer a threat is undetected in the network, the costs associated with a security breach increase.

3. **The cybersecurity skills gap is worsening** an already challenging hiring environment. As threats have evolved, cybersecurity requirements have increased. The U.S. government has outlined the NICE Framework, outlining 50+ security roles, demonstrating the increasing complexity organizations face when hiring in-house security staff.



Cyber Career Pathways Tool: https://niccs.cisa.gov/workforce-development/cyber-career-pathways.

50+ cybersecurity work roles are described within the Workforce Framework for Cybersecurity (NICE Framework), developed by the U.S. Government, as a free resource tool for the public, private, and education sectors in the United States.

The Challenges of **Operating a Modern-Day SOC**

To operate efficiently and effectively, SOCs need the right people, processes, and technologies, such as up-to-date threat intelligence systems. **They need to be staffed with enough analysts possessing the right capabilities** and experience to evaluate what artificial intelligence (AI) cannot.

Despite progress in automation technologies, every SOC still needs human intelligence, imagination, and experience to identify patterns and assess threat outliers that could indicate that an attack is underway. **An expanding attack surface**, an increase in total threats, and increasingly sophisticated obfuscation techniques, combined with the cybersecurity skills shortage, means most modern in-house, enterprise SOCs cannot fully react to the **growing complexity of security operations**.

A DAY IN THE LIFE OF A SECURITY ANALYST

A typical day in the life of a Security Analyst includes these responsibilities:

- **Monitoring the SIEM** for suspicious events and anomalous activity;
- **Investigating suspicious events** and incidents using open-source and proprietary intelligence sources;
- **Managing incident response**;
- **Tuning SIEM alerts** to improve detection engineering;
- **Keeping current with information** security news, techniques, and trends;
- **Monitoring log** collection activities;
- **Reporting any changes** in the security environments to the SOC Manager or CISO.
- **Notifying other critical stakeholders** of security incidents.

Some of the challenges today's enterprises face when it comes to Security Operations include:

- **Staffing shortages** (both lack of staffing both in quantity and skill level)
- **Alert fatigue and burnout**
- **Disparate security technologies**
- **Managing security compliance and risk**

Alert Fatique

Alerts arrive from disparate security tools, each with a limited scope within the environment, and therefore with a very limited ability to be contextualized before being logged. Inadequate ability to to efficiently correlate and filter these raw alerts risks inundated analysts with meaningless alerts, making it extremely difficult for them to identify the true positive needles in the proverbial haystack, the result is the problem known as alert fatigue.

Meaningful alerting is created by a useful mix of threat intelligence, indicators of compromise (IOCs) watchlists, machine learning, and automation in order to avoid this condition. This sophistication requires continuous adjustment and improvement in the alerting process.

Consequences of alert fatigue include:

- **Favoring or adjusting certain types** of alerts to reduce overall volume.
- **Ignoring certain alert** categories.
- **Ignoring alerts** in general because of the high false positive rate.

60% of businesses surveyed

SAID THE LACK OF SKILLED CYBERSECURITY PROFESSIONALS WAS PUTTING THEIR BUSINESS AT RISK.

- ISC² STUDY

The excessive number of alerts creates a series of additional problems by:

- **Contributing to analyst burnout**, as the daily onslaught of alerts eventually becomes too much to bear in an already stressful career.
- **Adding costs to the security team** and company, as skilled staff are taken away to work on more important tasks, instead of analyzing potential threats, and tuning security technologies to eliminate false positives.
- **Increasing the risk of an actual security incident** occurring due to the tendency of analysts to ignore alerts.

SOC Staffing Problems

Staffing a modern SOC can be difficult. An inadequately staffed SOC can be dangerous to business. The same (ISC)2 2021 study found 60% of businesses surveyed said the lack of skilled cybersecurity professionals was putting their business at risk.

Organizations attempting to staff their own SOC often struggle with the following challenges:

- **Maintaining optimal staffing** and creating an effective SOC staff structure.
- **Prioritizing roles** to ensure the right team is in place.
- **Balancing automation** with the right personnel.
- **Ensuring the SOC staffing** model has enough flexibility to scale.
- **Staffing for maturity** and future growth.
- **Providing career progression** with a limited budget and competitive hiring landscape.

Disparate Security Technologies

To cope with stretched security budgets and the inability to find skilled staff, businesses often decide to expand their security operations and SOCs by investing in more in-house security technology, like security information and event monitoring (SIEM) solutions and intrusion detection systems (IDS), incorrectly assuming that automation and AI and ML can somewhat augment for a lack of qualified staff. **Advanced technology still can't fully compensate** for the skills and expertise that an experienced cybersecurity professional can bring to SOC activities.

The addition of new technology can also serve to increase the burden on personnel. In the study **"The Life and Times of Cybersecurity Professionals 2021,**[3]**"** a cooperative research project by the **Enterprise Strategy Group** (ESG) and the **Information Systems Security Association** (ISSA), a third of the participants said that the skills shortage had created a scenario that prevented them from learning about or utilizing some of the company's security technologies to the fullest potential.

Security Compliance and Cybersecurity Risk Management

- **As organizations try to cope with increasing cyber risk**, governments and industry continue to build cybersecurity and data policy to protect both businesses and consumers. The increasing number of complex regulations and the risk of non-compliance fines puts pressure on enterprises to hire knowledgeable staff to facilitate security compliance and risks management concerns.
- **SOCs need to be staffed with individuals that understand** compliance issues and risk management processes and can monitor systems accordingly. The current staffing shortage makes it difficult for maturing businesses to adequately address regulatory, risk, and compliance concerns.

Bridging the Skills Gap **in Security Operations**

The bridge to improved security operations can be built in a number of ways.

Companies today can choose from one of the following three options:

- **Hire an in-house Security Operations team** and build an in-house Security Operations Center.
- **Hire an in-house team to work with a Managed Security Services Provider (MSSP)** for basic security service support.
- **Partner with a Managed Detection and Response (MDR)** provider for fully managed, outsourced 24/7/365 Security Operations experts and technology services.

TYPES OF SOCS

Depending on organizational need, different SOC structures may be useful:

- **Virtual SOC (VSOC)** Built on a decentralized structure with virtual teams
- **Multi-function SOC/NOC** Integrate security and network operations to improve communications, incident response, and incident management.
- **Co-managed SOC** Ideal for mid-sized companies with constrained budgets. Staffed and delivered by an MSSP/ MDR vendor.
- **Dedicated SOC** Built in-house with mature IT and security technology
- **Command SOC** Typically used by extremely large organizations providing shared services.

Most businesses do not have the resources necessary to build a modern SOC infrastructure and staff the full bench of security professionals they need to succinctly manage their unique security risks.

The next question then is **how much an organization wants to manage the day-to-day** complexity of their security operations program.

If an organization chooses an MSSP, the in-house team needs to be prepared, as managed services for real-time support may be limited. When a real-time incident occurs, real-time response may be limited to billable customer service hours conducted by off-shore call centers, **while escalated security alerts** may offer little to no data for the in-house team's investigation or documentation.

The option to partner with a Managed Detection and Response provider delivers value and provides cybersecurity at scale. In today's evolving landscape, this is a solid choice to secure the business with 24/7/365 security monitoring conducted by experts. **With the right MDR provider**, hard-to-hire experts provide eyes-on-glass around the clock to ensure anomalies in their customer's security environment are detected quickly. **If a true threat is identified**, the experts immediately contact the customer to coordinate rapid response activities to stop the threat fast and minimize financial impacts.

Benefits of Using MDR to Staff Your SecOps and SOC

Working with a Managed Detection and Response (MDR) provider can help businesses optimize the entirety of their security operations. **Outsourcing SecOps and SOC** activities to an MDR offers cost-effective benefits over attempting to manage security in house.

Working with an MDR provider to deliver security services can help:

Reduce Cybersecurity Costs Whether an organization is developing their overall security processes or wishing to build and maintain a SOC, these activities can be expensive—both in terms of staff and technology. An MDR provider can offer the expertise and latest technology solutions.

Reduce Alert Fatigue Through a combination of automated alert monitoring and analysis by expert staff, an MDR can reduce the burden on existing staff to investigate alerts.

Inventory Management An MDR provider can help SecOps and SOC teams inventory all endpoints and users on a network.

Ongoing Management and Maintenance of Security Tools SOCs require quite a few advanced technology tools—sometimes more than 20. MDR staff can support businesses by helping determine which tools to purchase, facilitating the purchasing process, and installing the technologies, then managing and maintaining the tools.

Benefits of Using MDR to Staff Your SecOps and SOC continued

Working with a Managed Detection and Response (MDR) provider can help businesses optimize the entirety of their security operations. **Outsourcing SecOps and SOC** activities to an MDR offers cost-effective benefits over attempting to manage security in house.

Incident Response An optimized SOC operates 24/7/365. An MDR provider can offer the SOC staff the support necessary to ensure no alert, anomaly, incident, or attack gets missed, particularly on holidays, weekends, or at night.

Improve Visibility MDR partners have the staff to provide 24/7/365 monitoring with the skill sets to analyze and correlate attacks across millions of transactions. Staff also possess the unique skills needed to identify sophisticated attacks during threat hunting activities.

Improve ROI MDR providers can help leverage existing technology solutions to improve ROI by maximizing the value of your existing tools.

Seamless integration MDR providers have the experience and expertise to integrate operations, staff, and additional technology solutions seamlessly with existing enterprise SEIM, vulnerability management, and active response.

Security Operations Staffing **for the Future**

The long working hours and increasing threat pressures placed on IT security decision makers and teams is not sustainable. Security leaders and business leaders need to work together to align funding resources that best maximize security investments and outcomes to secure and protect systems, users, and data from harm.

To cope with both staffing and budget challenges, **the most efficient and cost-effective way to manage the increasing proliferation of threats** and attacks is through a fully functioning and staffed SecOps team and SOC that has the built-in capability to scale for both business growth and evolving threats. By working with a trusted **Managed Detection and Response** provider, organizations can scale investments and security maturity with an expert staff for **24/7/365** threat detection and incident response. This choice covers the organization for business continuity in the short-term, and strengthens security maturity over time to secure the future of the business in the long-term.

deepwatch

ABOUT DEEPWATCH'S MANAGED DETECTION & RESPONSE SERVICES

Deepwatch is a trusted security leader, offering professional and innovative managed security to help support security operations and stop breaches and attacks. Deepwatch's managed detection and response services include 24/7/365 threat monitoring, alerting, validation, and proactive threat hunting, with accelerated detection of malware, botnets, and ransomware behavior aided by industry's most comprehensive and fastest platform built with machine learning and content libraries. At Deepwatch, organizations work with a named squad—an assigned team of experts that includes detection and response analysts and threat hunters who take time to understand a business's unique environment.

Deepwatch secures enterprises via its unique, highly automated cloud based SOC platform backed by a world class team of experts that protect your network and digital assets 24/7/365. Deepwatch extends your team and proactively improves your cybersecurity posture via our proprietary maturity model. Deepwatch's managed security services are trusted by leading global organizations.

Visit www.www.deepwatch.com or reach out to us at sales@www.deepwatch.com.

SOURCES

[1] (ISC)² Cybersecurity Workforce Study, 2021: A Resilient Cybersecurity Profession Charts the Path Forward; https://www.isc2.org/Research/Workforce-Study#

[2] Overworked CISOs are Skipping Family Vacations and Holidays; https://www.infosecurity-magazine.com/news/overworked-cisos-are-skipping/

[3] ESG RESEARCH REPORT, The Life and Times of Cybersecurity Professionals 2021, Volume V, A Cooperative Research Project by ESG and ISSA; https://www.issa.org/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf

National Initiative for Cybersecurity Careers and Studies (NICCS) Workforce Framework for Cybersecurity (NICE Framework), https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

Verizon 2021 Data Breach Investigations Report; https://www.verizon.com/business/resources/reports/dbir/

(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide; https://www.isc2.org/News-and-Events/Press-Room/Posts/2019/11/06/ISC2-Finds-the-Cybersecurity-Workforce-Needs-to-Grow--145